Poster

Noise-Free Security Assessment of Eviction Set Construction Algorithms with Randomized Caches

Amine Jaamoum
CEA, LETI MINATEC Campus, University Grenoble Alpes, 38054 Grenoble, France
amine.jaamoum@cea.fr

Thomas Hiscock
CEA, LETI MINATEC Campus, University Grenoble Alpes, 38054 Grenoble, France
thomas.hiscock@cea.fr

Giorgio Di Natale
CNRS, Grenoble INP, TIMA, University Grenoble Alpes, 38000 Grenoble, France
giorgio.di-natale@univ-grenoble-alpes.fr

Cache timing attacks, i.e., a class of remote side-channel attack, have become very popular in recent years. Eviction set construction is a common step for many such attacks, and algorithms for building them are evolving rapidly. On the other hand, countermeasures are also being actively researched and developed. However, most countermeasures have been designed to secure last-level caches and few of them actually protect the entire memory hierarchy. Cache randomization is a well-known mitigation technique against cache attacks that has a low-performance overhead. In this study, we attempted to determine whether address randomization on first-level caches is worth considering from a security perspective. In this paper, we present the implementation of a noise-free cache simulation framework that enables the analysis of the behaviour of eviction set construction algorithms. We show that randomization at the first level of caches (L1) brings about improvements in security but is not sufficient to mitigate all known algorithms, such as the recently developed Prime–Prune–Probe technique. Nevertheless, we show that L1 randomization can be combined with a lightweight random eviction technique in higher-level caches to mitigate known conflict-based cache attacks.

Keywords: *cache side-channel attacks; address randomization; eviction set construction; security; Micro-architecture*